CMPT 424.3 FINAL EXAMINATION

December 17th, 2003

Total Marks: 100

CLOSED BOOK and CLOSED NOTES
NO CALCULATOR

Time: 3 hours

Instructions

Read each question carefully and write your answer legibly on the examination paper. **No other paper will be accepted.** You may use the backs of pages for rough work but all final answers must be in the spaces provided. The marks for each question are as indicated. Allocate your time accordingly.

Ensure that your name AND student number are clearly written on the examination paper and that your name is on every page.

Question	Marks
1 (10 marks)	
2 (12 marks)	
3 (9 marks)	
4 (15 marks)	
5 (15 marks)	
6 (15 marks)	
7 (12 marks)	
8 (12 marks)	
Total	

Name: _____

Student Number: _____

Student Number:_____

1. **General** (*10 marks*) Give the technical term that best fits each of the following descriptions or definitions.

   (a) A type of network service in which a packet can be sent to multiple recipients with a single "send" operation.

   (b) A data structure that binds a public key to a particular entity, and that is digitally signed by a trusted third party.

   (c) A traffic "policing" mechanism that can be used to regulate a packet flow's average rate, peak rate, and burst size.

   (d) The method used by TCP to average the measured round-trip times between a sender and receiver.

   (e) A standard for interconnecting computing and communication devices and accessories (such as cordless phones and PDAs) using short-range, low power, inexpensive wireless radio.

   (f) A type of packet-switched network in which each packet carries the address of the destination host. Packets from the same flow may take different paths through the network.

   (g) A protocol suite that provides security at the network layer.

   (h) The multiple access protocol used in IEEE 802.11.

   (i) A theorem that bounds the achievable data rate on a noiseless channel of bandwidth H.

   (j) An organization with many servers distributed throughout the Internet, at which Web objects of its customers are replicated, and from which these objects are served to nearby requesting clients.

Student Number:_____

2. **Network Architecture** (*12 marks in total*)

(a) (*6 marks*) If one captured the network traffic on a campus Ethernet segment, one would find a wide variety of network protocols to be in use. Each protocol (except those at the bottom of the protocol stack) uses some different protocol to carry its messages as payload. For example, UDP segments are carried in IP packets. For each of the other protocols given in the table below, give the protocol that you would expect it to be using.

Protocol	Next Lower Protocol
UDP	IP
DNS	
FTP	
SSL	
ICMP	
RTCP	
ARP	

(b) (*6 marks*) Each of the following parts concerns layered network architectures.

(i) Define the terms *protocol* and *interface*, as used in the context of layered network architectures.

(ii) What are the principal benefits of using a layered architecture?

(iii) What might be the drawbacks of using a layered architecture with many layers?

3. **Application Layer** (*9 marks in total*)

    (a) (*6 marks*) The HTTP protocol is stateless, and yet Web sites are able to keep track of user identity when required (for example, across successive requests to a secure web site, or when maintaining a user's shopping basket at an e-commerce site). Define what is meant by the term *stateless* in this context, and then describe *two* distinct methods by which web sites can keep track of user identity across successive requests to the same site.

    (b) (*3 marks*) SMTP, IMAP, and POP3 are all protocols concerned with the provision of email services. State the purpose of each protocol.

Student Number:_____

4. **Transport Layer** (*15 marks in total*)

(a) (*3 marks*) In Bluetooth, frames have a 1 bit sequence number field. What does this tell you about the Bluetooth reliable data transfer protocol? Explain your answer.

(b) (*3 marks*) What information is used at a host to *demultiplex* incoming TCP segments?

(c) (*3 marks*) How does *TCP Reno* differ from *TCP Tahoe*?

(d) (*6 marks*) Outline the protocol by which a TCP connection is closed.

Student Number:_____

5. **Network Layer** (*15 marks in total*)

    (a) (*3 marks*) The size of an IP address in IPv4 is only 32 bits, and given the rate of growth of the Internet and the uneven allocation of the address space, running out of addresses is a potentially major concern. State the existing approaches for dealing with this problem.

    (b) (*3 marks*) What new requirements lead to use of a different algorithm for *inter-domain* Internet routing, than for *intra-domain* routing?

    (c) (*3 marks*) Outline how an Internet router uses its routing table to determine where to forward an incoming packet.

    (d) (*6 marks*) Outline the *indirect routing* approach to communicating with a mobile node.

6. **Data Link Layer** (*15 marks in total*)

   (a) (*6 marks*) Consider an error correction scheme in which the m data bits of a message are copied k times, yielding a "codeword" of length mk.

        (i)   What is the resulting Hamming distance?

        (ii)   For at most how many single bit errors can error correction be guaranteed?

        (iii)   Suppose that the data bits are $d_1d_2...d_m$, and that $k=3$.   Should the codeword be constructed as $d_1d_1d_1d_2d_2d_2...d_md_md_m$, or as $d_1d_2...d_md_1d_2...d_md_1d_2...d_m$? Explain.

   (b) (*6 marks*) Some data link layer protocols require the receiver to acknowledge each frame, with the sender retransmitting if an acknowledgement is not received, while others rely on upper layer protocols (e.g., TCP) to retransmit data as required. Describe the advantages and disadvantages of these two approaches, and the contexts in which each might be preferable.

   (c) (*3 marks*) Ethernet specifies a minimum frame size, implying that if a frame contains only a small amount of data, the data must be padded so that the minimum size is achieved. Why does Ethernet impose this restriction?

Student Number:_____

7. **Multimedia Networking** (*12 marks in total*)

  (a) (*6 marks*)   Unlike other Web content such as text and images, video files are often *not* delivered using HTTP. Explain what disadvantages HTTP has in this context.

  (b) (*6 marks*) Outline the *integrated services* and *differentiated services* approaches to providing quality of service in the Internet, stating the advantages and disadvantages of each.

8. **Security** (*12 marks in total*)

   (a) (*6 marks*) Give the current advantages and disadvantages of *public key* cryptography in comparison to *symmetric key* cryptography.

   (b) (*6 marks*) Outline a protocol of minimal complexity by which two entities "Alice" and "Bob" can establish a shared secret key K_{A-B}. Assume that Alice and Bob each know each other's public key. Your protocol must guard against replay attacks.

The End